COGITATIO

**Media and Communication (ISSN: 2183-2439)**
**2015, Volume 3, Issue 2, Pages 53-62**
**Doi: 10.17645/mac.v3i2.297**

Article

# EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era

Nora Ni Loideain

Faculty of Law, University of Cambridge, Cambridge, CB3 9DZ, UK; E-Mail: nl301@cam.ac.uk

Submitted: 18 April 2015 | Accepted: 17 June 2015 | Published: 30 September 2015

**Abstract**
Legal frameworks exist within democracies to prevent the misuse and abuse of personal data that law enforcement authorities obtain from private communication service providers. The fundamental rights to respect for private life and the protection of personal data underpin this framework within the European Union. Accordingly, the protection of the principles and safeguards required by these rights is key to ensuring that the oversight of State surveillance powers is robust and transparent. Furthermore, without the robust scrutiny of independent judicial review, the principles and safeguards guaranteed by these rights may become more illusory than real. Following the Edward Snowden revelations, major concerns have been raised worldwide regarding the legality, necessity and proportionality standards governing these laws. In 2014, the highest court in the EU struck down the legal framework that imposed a mandatory duty on communication service providers to undertake the mass retention of metadata for secret intelligence and law enforcement authorities across the EU. This article considers the influence of the Snowden revelations on this landmark judgment. Subsequently, the analysis explores the significance of this ruling for the future reform of EU law governing metadata surveillance and its contribution to the worldwide debate on indiscriminate and covert monitoring in the post-Snowden era.

**Keywords**
Edward Snowden; EU law; human rights; judicial review; mass surveillance; metadata; personal data; privacy

**Issue**
This article is part of the special issue "Surveillance: Critical Analysis and Current Challenges", edited by James Schwoch (Northwestern University, USA), John Laprise (Independent Researcher) and Ivory Mills (Northwestern University, USA).



## 1. Introduction

Laws within democratic states prohibit public authorities from looking into the private lives of their citizens merely because they have the technological capacity to do so. The right to respect for private life and the protection of personal data underpin such national legal frameworks within the European Union (EU). Accordingly, the protection of this human right is key to ensuring that the oversight of State powers that permit the covert surveillance of communications for legitimate purposes (such as the prevention of terrorism and serious crime) is adequate and transparent. Moreover, without the robust scrutiny of independent judicial review, the principles and safeguards that ensure the effective application of this human right are at risk from becoming more illusory than real. Following the Edward Snowden revelations, major concerns were raised worldwide regarding the legality, necessity and proportionality standards governing State surveillance powers (Greenwald, 2014; Harding, 2014). Shortly thereafter in 2014, the highest court in the EU struck down the legal framework that imposed a mandatory duty on communication service providers to undertake the mass retention of their customers' metadata for up to two years in case this information may have assisted in the investigation, detection and prosecution of serious crime (Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger*). This article considers the influence of the Snowden revelations on this landmark judgment. The analysis begins by addressing the key factors that have contributed to the increasing importance of metadata for modern State surveillance. This examination then outlines the principles and safe-

guards guaranteed by the right to respect for private life under Article 8 of the international human rights instrument of the European Convention on Human Rights (ECHR) that apply to the covert surveillance of metadata by public authorities within the EU. The analysis thereafter discusses the origins, main provisions and controversy surrounding the legal framework that entrenched the mass and indiscriminate retention of metadata across the EU (section 2). Next, the article provides a brief overview of the Edward Snowden revelations with a focus on the covert mass metadata surveillance regime uncovered therein (section 3). The analysis subsequently turns to the main findings of the landmark judgment of the Court of Justice of the EU (CJEU/Luxembourg Court), the role of the Snowden revelations and the implications of this ruling for the EU legal order and data protection policy developments both within and beyond the EU (section 4). Lastly, the article concludes with a brief summary (section 5).

## 2. Metadata Surveillance

### *2.1. What Is Metadata Surveillance?*

The term "metadata" relates to information generated or processed as a consequence of a communication's transmission. Much can be revealed from this data including: "latitude, longitude and altitude of the sender's or recipient's terminal, direction of travel…any naming, numbering or addressing information, volume of a communication, network on which the communication originates or terminates, and the beginning, end or duration of a connection" (Young, 2004). Metadata therefore concerns the *context* as opposed to the content of a communication and covers many types of information such as traffic data, location data, user data and the subscriber data of the device/service being used (e.g. cellular phone network or Internet service provider). As a result, metadata is a rich source of personal information as it reveals the "who" (parties involved), the "when", how long and how often, (time, duration and frequency), the "what" (type of communication, e.g. phone call, message, e-mail), the "how" (the communication device used, e.g. landline telephony, smartphone, tablet) and the "where" (location of devices used) involved in every communication we make. Moreover, the collection, aggregation and analysis of metadata can provide very detailed information regarding an individual's beliefs, preferences and behaviour.

In the 21st century, the depth and breath of information concerning an individual's private life that can now be revealed through the metadata surveillance of communications have advanced in tandem with dramatic technological developments.

Of particular note in this respect are two major changes regarding how society now communicates. First, there has been a distinct shift in the past century from the prevailing use of non-portable devices such as landline phones, faxes and personal computers to handheld smartphones and tablets. Secondly, major advancements in digitization and Internet access has led to the convergence of all of our communications (calls, e-mails, web searches, online shopping) to one device that is both mobile and Internet-enabled (Wicker, 2013). The constant trail of metadata left behind from the ceaseless use of these so-called "smart" communications devices facilitates the collection of unprecedented amounts of data and presents unique privacy challenges. As highlighted by the US Federal Trade Commission (FTC), "more than other types of technology, mobile devices are typically personal to an individual, almost always on, and with the user" (FTC, 2013).

Furthermore, given the increasingly ubiquitous use of mobile communication devices, these changes have made metadata surveillance just as valuable as (if not more than) the *content* of your communications for both law enforcement and commercial purposes. Consequently, the collection and processing of an individual's metadata can provide a level of monitoring of an individual's every communication and movement that was never attainable previously. For instance, Malte Spitz, a German Green Party representative, demonstrated the scope of this surveillance in a request to his mobile phone provider. Spitz sought a record of all the metadata collected and retained from the use of his mobile phone. Over the course of six months, this metadata tracked his geographical location and the use of his phone more than 35,000 times building a detailed narrative of his movements and his communications (Spitz, 2012). In other words, access to the content of our communications is no longer necessary to show what and whom we're interested in and what's important to us (Schneier, 2015).

### *2.2. Metadata Surveillance Threatens Privacy, Equality and Liberty*

Unquestionably, the major technological developments outlined above have made the monitoring of metadata an essential and important tool for national security and law enforcement authorities around the world. The value of this surveillance was confirmed by General Michael Hayden, former director of the US National Security Agency (NSA) and the Central Intelligence Agency (CIA), who noted in a public debate concerning privacy and the NSA: "We kill people based on metadata" (Hayden, 2014).

However, indiscriminate mass metadata surveillance of entire populations by governments generates abundant amounts of personal data and consequently represents a substantial threat to the privacy, equality and liberty of individuals. This information can often be sensitive in nature and may identify many aspects of an individual's private life, including personal and profes-

sional relationships, racial or ethnic origin, political affiliations, religious beliefs, trade-union membership, financial status or medical history, to name just a few. The subsequent "aggregation" of this data into comprehensive online dossiers can reveal more to governments and private industry about an individual's identity and behaviour, than the individual may ever be aware of (Solove, 2008).

Accordingly, the creation, access and dissemination of such detailed digital profiles could result in insidious threats of computer-enhanced discrimination and manipulation that ought to raise considerable concern. The groups that face exclusion from access to opportunities (e.g. employment), goods or services based on data obtained from their Internet usage (particularly e-mail and web browsing) are less likely to be aware of their status as victims of categorical discrimination (Lessig, 1999). As a result, they will be even less likely to organize as an aggrieved group in order to challenge their exclusion from opportunities provided by the State or private sector (Gandy, 2003), thereby being prevented from asserting their constitutionally protected rights to privacy, equality and liberty.

### *2.3. Metadata Surveillance and the European Convention on Human Rights*

Contracting States to the international human rights instrument of the European Convention on Human Rights (ECHR), who are also Member States of the EU, have argued in the past that the intrusion posed by metadata surveillance represents nothing more than a minimal interference with an individual's right to respect for private life (Ni Loideain, 2014a). However, since its leading judgment of *Malone* v. *United Kingdom* delivered in 1984, the European Court of Human Rights in Strasbourg (the international court established under the ECHR which reviews challenges to violations of the ECHR by Contracting States) has rejected this assertion.

Instead, the Strasbourg Court has consistently held that any processing (e.g. retention, access, analysis, storage, third-party dissemination) of metadata from an individual's communications (including telephony, e-mail, Internet usage) constitutes an interference with the right to respect for private life, as guaranteed under Article 8 of the ECHR. Moreover, the Strasbourg Court has subsequently upheld a number of challenges (*Valenzuela Contreras* v. *Spain* (1999); *Copland* v. *United Kingdom* (2007); *Liberty* v. *United Kingdom* (2009)) regarding the illegal use of these covert metadata surveillance powers by Contracting States. As will be examined below (see section 4.1), the highest court in the EU (CJEU/Luxembourg Court) would later close ranks with the approach of the Strasbourg Court in its landmark post-Snowden judgment of Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger*. The Luxembourg Court would do so by striking down an EU law that had raised human rights concerns within EU institutions and national courts across Europe since its inception.

### *2.4. Mass Metadata Surveillance and EU Law*

Under the weight of considerable political pressure for increased counter-terrorism powers that followed the 9/11 attacks and the Madrid and London bombings in 2004 and 2005, the Data Retention Directive (2006/24/EC) was rapidly drafted, passed and entered into force by the EU legislature in 2006 (Murphy, 2012; Ni Loideain, 2011). The Directive provided that metadata derived from the communications of every natural person and legal entity within the EU must be retained and made available for the purpose of "the investigation, detection and prosecution of serious crime", as defined by each Member State in its national law. Specifically, this blanket measure imposed a mandatory duty on Member States to require private communication service providers to store and facilitate access to all of their customers' metadata to competent national authorities for up to two years. Under the 2006 EU Directive, this metadata concerned the devices used, the type of communication, the parties involved, their locations and the times and frequency of their communications. The broad scope of the Directive encompassed metadata from landline and mobile telephony, Internet access, Internet telephony and e-mail.

The EU legislature stated that the aim of the Data Retention Directive was to harmonize the varying domestic laws of EU countries concerning the retention of certain metadata by the private sector in order to ensure the availability of this information for the investigation, detection and prosecution of serious crime, as defined by each country under their national law. Nevertheless, many representatives of the EU Parliament, data protection authorities and NGOs across the EU consistently contested the compatibility of the Data Retention Directive with Article 8 of the ECHR and the EU Charter of Fundamental Rights. The EU Charter, effectively the EU's Bill of Rights, affirms the commitment of the EU to human rights and governs EU institutions and Member States when they are "implementing" EU law (EU Charter, Art.51(1)). Therefore, the scope of the EU Charter's application is much more narrow when compared to the US Bill of Rights as it does not impose a "federal standard" against which all national laws of the 28 Member States within the EU may be evaluated and set aside (Groussot & Pech, 2010).

The decision of the EU legislature to allow EU Member States to require the private sector to retain their customers' metadata for up to two years raised particularly major concerns. Previously, communication service providers would only keep this personal data for six months on average for billing purposes. There

would have been some exceptions where information was held for longer if needed for the purpose of national security (Hawkes, 2006). Under the EU Data Retention Directive, however, storing this personal data for longer than six months was no longer the exception. Strikingly, no empirical evidence was put forward by any of the EU institutions to justify such a significant departure from the well-established principles of EU data protection law, particularly the tenet that personal data be retained for specific purposes within a scope that is necessary and proportionate. Even the Impact Assessment Report prepared by the European Commission, which served as the basis for proposing the Data Retention Directive, indicated that an upper maximum limit of only *one year* would be appropriate (European Commission, 2005). The Report warned that "a longer retention period would appear to be of little added value for law enforcement authorities while having important financial consequences for operators and [infringing] disproportionately on citizens' privacy".

Prior to its review by the CJEU in 2014, many of the highest national constitutional courts across the EU (Bulgaria, Cyprus, Czech Republic, Germany and Romania) had already upheld challenges striking down national provisions implementing the EU Data Retention Directive. The main grounds underpinning these judgments concerned the surveillance regimes' inadequate oversight and security standards and overall incompatibility with the legality, necessity and proportionality requirements mandated by the right to respect for private life, as guaranteed under Article 8 of the ECHR (Ni Loideain, 2014b).

## 3. The Snowden Revelations and Metadata Surveillance

Edward Snowden is a US citizen who now has temporary residence in Russia. He is a former computer analyst for the CIA and was subsequently employed as a defense consultant with *Booz Allen Hamilton*—a private management and technology consulting company contracted by the NSA. In June 2013 in Hong Kong, Snowden released thousands of US government records collected in his capacity at *Booz Allen Hamilton* revealing details of several programmes involving the mass surveillance of communications belonging to individuals both within and outside of the US to a select group of journalists in the UK and US news media, mainly *The Guardian* and *Washington Post* (Greenwald, 2014; Harding, 2014). Subsequently, news media outlets worldwide have also highlighted the questionable legality of US national security authorities sharing personal data obtained from these large-scale monitoring regimes with government authorities outside of the US (Article 29 Data Protection Working Party, 2014).

Among the many types of covert surveillance regimes that became public knowledge following the Snowden revelations, it came to light that one particular programme had been in operation for more than seven years. Similar to the EU Data Retention Directive, this monitoring involved the mass retention and access to metadata from the use of mobile phones for national security and law enforcement purposes. Following a court order issued under the Foreign Intelligence Surveillance Act 1978 (FISA), as amended, the Foreign Intelligence Surveillance Court required *Verizon* (one of the largest US communication service providers) to provide millions of phone records concerning its US customers on a daily basis to the NSA. This order included the telephony metadata of both US and non-US citizens as it applied to communications "(i) between the United States and abroad"; or (ii) wholly within the United States, including local telephone calls" (FISA Order, 2013). Although the duration of the FISA order was only for a three-month period, the same order had been the subject of renewal for seven years.

The revelations have prompted an ongoing global debate concerning the rapid pace of technological developments in the area of communications surveillance and the implications posed by this large-scale secret monitoring for individual's rights to privacy and the security of their personal data (Kuner et al., 2015). Furthermore, the revelations have also drawn attention to the significant role played by the private sector in the mass surveillance of communications for governments. Of notable controversy recently has been the question of whether governments should have a "back door" to the encrypted communications of the customers belonging to these private companies (Hayden, 2015). This issue has raised major concerns regarding the extent to which private actors should be co-opted into the blanket monitoring of individuals' communications for governments.

The subsequent complex debate on future law reform has resulted in a diverse range of responses from legal academics, the judiciary and the communication services industry in the EU and US. For example, in a report by the Review Group on Intelligence and Communications Technologies commissioned by US President Obama, the authors recommended that the bulk retention of metadata for State surveillance purposes should be the responsibility of communication service providers or other third-party private actors (The President's Review Group on Intelligence and Communications Technologies, 2013). In their view, storage by the government of bulk metadata creates potential risks to public trust, personal privacy, and civil liberty. However, the Grand Chamber of the highest court in the EU held the opposite in the landmark judgment of *Digital Rights Ireland and Seitlinger* shortly thereafter in April 2014. The CJEU struck down the 2006 EU Data Retention Directive for being in breach of the EU Charter of Fundamental Rights. As examined above (see section 2.4), this impugned EU law had imposed a mandatory

obligation on all Member States of the EU several years earlier to require private communication service providers to retain the metadata of their customers for the investigation, detection and prosecution of serious crime for up to two years.

## 4. The Post-Snowden Era and the Landmark Judgment of the CJEU

### *4.1. Digital Rights Ireland and Seitlinger*

The landmark judgment of *Digital Rights Ireland and Seitlinger* responded to requests from the High Court of Ireland and the *Verfassungsgerichthof* (Constitutional Court) of Austria that the CJEU examine the validity of the EU Data Retention Directive, particularly its compliance with the EU Charter of Fundamental Rights. Due to this metadata surveillance regime being an area of EU law, these courts were required to refer to the Luxembourg Court. EU law provides that national courts of EU Member States are unable to rule on the validity of EU legislation and therefore the constitutional courts of Ireland and Austria could not review the legality of the 2006 EU Directive (Case C-314/85 *Foto-Frost* v. *Hauptzollamt Lübeck-Ost* [1987] ECR 4199). Both proceedings arose from challenges to invalidate the national laws that implemented the EU Directive into Austrian and Irish law. Given the overlap of issues raised between the cases, the CJEU issued a joined response to both national courts. In a notable reflection of the reservations held by EU citizens towards this mass and indiscriminate retention of metadata, the reference to the CJEU from the *Verfassungsgerichthof* was the result of a constitutional challenge brought by more than 11,000 applicants (De Vries et al., 2011).

On 8 April 2014, the Luxembourg Court (sitting as a Grand Chamber of fifteen judges), seems to have acknowledged the human rights concerns raised by the national courts, data protection authorities and NGOs across Europe, by holding that the Data Retention Directive was invalid under EU law. The Court recognised the growing importance of metadata surveillance as "a valuable tool" for criminal investigations (para. 43 of the judgment). Nevertheless, the Court made clear that interfering "with the fundamental rights of practically the entire European population" for the legitimate objective of tackling serious crime does not justify surveillance regimes of the indiscriminate and unreasonable nature permitted under the Directive (para. 56). The Court criticized the starkly indiscriminate and therefore disproportionate scope of the Directive given that it applied to "all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime" (para. 56).

In particular, the Court took issue with the length of the retention period, that access by law enforcement authorities to data retained under the Directive did not depend on prior approval by a judge or another independent body and that the Directive did not explicitly require that Member States ensure that the private sector provide a high level of protection and security for the retained data (para. 66). The Court also highlighted that the Directive did not ensure the "irreversible destruction" of the data at the end of the retention period (para. 67). Additionally, in an uncharacteristic departure from its traditional minimalist approach, the Court addressed an issue that was not referred by either of the national constitutional courts. Specifically, the Court raised concerns regarding the location of the data retention under the fundamental right to protection of personal data guaranteed by Article 8 of the EU Charter. The Court held that the metadata retained under the Directive should have remained within the EU in order to fully ensure, as required under Article 8(3), the control "by an independent authority of compliance with the requirements of protection and security" (para. 68).

Based on all of the above grounds, the Court held that the "EU legislature had exceeded the limits imposed by compliance with the principle of proportionality" guaranteed under the fundamental rights to respect for private life and the protection of personal data under Articles 7, 8 and 52 of the EU Charter of Fundamental Rights (para. 69). By not limiting the temporal effect of its judgment, the Court declared the invalidity of the Directive to take effect *ab initio* (from the beginning), thereby erasing its entire existence from the EU legal order.

### *4.2. The Influence of the Snowden Revelations*

Unquestionably, *Digital Rights Ireland and Seitlinger* is a landmark judgment likely to have reassured national courts of the EU's commitment to fundamental rights. The judgment has also been lauded for confirming that high standards of privacy and data protection apply to the mass processing of personal data within the EU (Guild & Carrera, 2014; Lynskey, 2014). Despite the implications for other EU counter-terrorism policies, by invalidating the entire existence of the Data Retention Directive due to its incompatibility with the EU Charter, the Court "confirmed its commitment to an advanced system for the protection of human rights even in the context of national security" (Fabbrini, 2014). Furthermore, this is the first time that the highest Court in the EU has ever struck down an entire EU legal instrument due to its incompatibility with the EU Charter of Fundamental Rights.

Moreover, to the surprise of many, the Luxembourg Court in *Digital Rights Ireland and Seitlinger* also made a novel and major contribution to the EU legislative framework governing data protection, and for any fu-

ture EU data retention measures. Notably, the Court appears to have effectively established that "data sovereignty' is a key element of the right to the protection of personal data guaranteed under Article 8 of the EU Charter of Fundamental Rights. Without this element, the Court stressed, the control by an independent supervisory authority of ensuring compliance with necessary data protection and data security requirements, required under Article 8 of the EU Charter, cannot be fully ensured. Strikingly, the Court did not limit the scope of this interpretation of Article 8(3) of the EU Charter to data retained under EU law for the purposes of tackling terrorism and serious crime, thereby making this requirement applicable to the retention of data pursuant to *any* EU legal measure. Accordingly, some commentators have gone as far as to note that the judgment could be interpreted as preventing the transfer of personal data to non-EU private and public bodies since access and use of this information would then be removed from the control of an independent supervisory authority, contrary to EU fundamental rights (Granger & Irion, 2014).

Consequently, the potential policy implications of the CJEU's interpretation of Article 8 of the EU Charter in *Digital Rights Ireland and Seitlinger* for the ongoing reform of EU data protection law are of considerable significance to public and private bodies both within the EU and beyond. By engaging so forcefully with an issue not referred by either of the national constitutional courts or decisive to the judgment, the Court's initiative in making this policy recommendation strongly suggests that the Snowden revelations played a role in the Court's assessment of the Data Retention Directive. While concerns relating to the need for data sovereignty between the EU and the US can be traced back to the 1970s, the emergence of the Snowden revelations has undoubtedly given impetus to a global debate on jurisdictional restrictions and the flow of personal data (Kuner, Cate, Millard, Svantesson, & Lynskey, 2015). To explicitly include a requirement of physical data retention within the EU under the EU Charter may result in major revisions to current provisions and exemptions under EU data protection law. In particular, such a requirement raises questions regarding the processing of data by the private sector and law enforcement authorities outside of the EU—a matter shortly to be before the Luxembourg Court in its review of the EU-US Safe Harbor Agreement.

### *4.3. Implications for the EU Legal Order and Beyond*

A consensus among EU Internet regulation policymakers and scholars has emerged that the Snowden revelations have been influential in "emboldening" the approach of the highest court in the EU in its review of matters concerning privacy and data protection (Centre for European Legal Studies, 2015). Two landmark judgments delivered in the post-Snowden era by the CJEU support this contention.

First in April 2014 (as examined above), the CJEU struck down the entire legal existence of an EU law in *Digital Rights Ireland and Seitlinger* that entrenched a regime of mass metadata surveillance across the EU on the ground that it was incompatible with the EU Charter of Fundamental Rights. Furthermore, the highest court in the EU also surprised EU privacy scholars in its adjudication that data sovereignty forms part of the right to the protection of personal data guaranteed under Article 8 of the EU Charter of Fundamental Rights.

Secondly, shortly thereafter on 13 May 2014, the Grand Chamber of the Court delivered a second landmark privacy judgment where it established that EU citizens have a right to have links concerning them delisted from search engines that essentially encroach upon their private lives and the protection of their personal data (Case C-131/12 *Google Spain* v. *AEPD and Mario Costeja Gonzalez*). Specifically, the Court recognized a right under the 1995 EU Data Protection Directive (95/46/EC) for individuals to remove links generated by Internet search engines concerning searches for an individual's name which produce results that are "inadequate, irrelevant or no longer relevant, or excessive" (para. 92 of judgment). While the focus of *Google Spain* was not directly concerned with State surveillance, it nevertheless reaffirms the emboldened stance of the CJEU in matters affecting EU citizens' fundamental rights to respect for their private life and the protection of their personal data in the post-Snowden era.

Unlike the much-lauded *Digital Rights Ireland and Seitlinger*, however, it is important to note that *Google Spain* has divided academics, policymakers and the communication services industry worldwide. Some have gone so far as to describe the ruling as an infringement to the rights of access to information, freedom of expression and freedom of speech as it "opens the door to large scale private censorship in Europe" (CCIA, 2014). Others have argued that the practical impact of the so-called "right to be forgotten" (more accurately, the right to be delisted) will be comparatively limited in scope given the removal by search engines of links that involve millions of copyright violations on a monthly basis (Mayer-Schonberger, 2014). Notwithstanding the aforementioned concerns, it is important to highlight that *Google Spain* was an (albeit ill-conceived) attempt by the Court to address two important problems for the protection of privacy in the 21st century. First, "the Internet's ability to preserve indefinitely all its information about you, no matter how unfortunate or misleading" (Zittrain, 2014) and secondly, the enormous influence of search engines regarding your online (and inevitably offline) identity and reputation.

Unquestionably, however, both of these striking decisions delivered by the Luxembourg Court concerning the protection of the right to respect for private life

and the protection of personal data since the Snowden revelations have strengthened the protection afforded by these human rights under EU law. The influence of the revelations for the protection of privacy through judicial review in Europe may extend further still in the future, given a pending application before the European Court of Human Rights in Strasbourg and in another related judgment pending before the CJEU in Luxembourg.

Both of these forthcoming human rights challenges concern the surveillance of personal data for national security and law enforcement purposes. The ongoing proceedings before the Strasbourg Court, *Big Brother Watch and Others* v. *United Kingdom* (App.58170/13), have been brought by three NGOs and Dr Constanze Kurz who allege that they may have been subject to surveillance by UK national security authorities in receipt of foreign intercepted material relating to their electronic communications. The applicants submit that this monitoring system (made possible by the PRISM, UPSTREAM and TEMPORA programmes revealed by Edward Snowden) violates their right to respect for private life, as guaranteed under Article 8 ECHR. In particular, the applicants assert that the requirements under the legality condition of Article 8 ECHR have not been satisfied by the UK legislature given that there is no statutory regime governing such surveillance and therefore there is an absence of adequate safeguards. Furthermore, the applicants contend that the "generic interception" of these external communications, merely on the basis that such communications have been transmitted by transatlantic fibre-optic cables, is an inherently disproportionate interference with the private lives of thousands, perhaps millions, of people.

The second set of proceedings pending before the CJEU in Luxembourg involves an Austria-based NGO (*Europe v Facebook*) which requested that the Data Protection Commissioner of Ireland issue proceedings against Apple and Facebook (both US companies have their European headquarters in Dublin) for violating EU data protection law by providing the personal data of EU citizens to the NSA. However, the then Commissioner, Mr Billy Hawkes, declined on the basis that both companies were parties to the Safe Harbor Agreement. This Agreement is a self-regulatory framework enforced by the US FTC and governs the exchange of personal data between the EU and US, thereby allowing US law enforcement authorities to access this information within the US. The Commissioner's decision was then challenged before the High Court of Ireland. Due to the implications of this judgment for the legal validity of the EU Data Protection legal framework, the national constitutional court referred the matter to the CJEU where oral hearings were held in March 2015. Specifically, the Irish High Court noted that the critical issue for the CJEU to determine concerns the interpretation of the 1995 EU Data Protection Directive and the decision by the European Commission in 2000 that under the Safe Harbor Agreement the US provides an adequate level of data protection. Both of these frameworks were drafted decades before social media became the increasingly ubiquitous form of communication that it is today, long before companies such as Facebook ever existed and before the EU Charter of Fundamental Rights became law in 2009. In light of the latter development, the Irish High Court seeks clarification from the CJEU regarding whether the 1995 EU Directive and the 2000 Commission's Safe Harbor Decision should be re-evaluated given the fundamental right of EU citizens to the protection of their personal data as guaranteed under Article 8 of the EU Charter (Case C-362/14 *Schrems* v. *Data Protection Commissioner*). It will be significant to see whether the Luxembourg Court will endorse the ongoing work of the EU legislature to reform and update the current Safe Harbor Agreement with the US Government (Kuner, 2015). Alternatively, the CJEU may adopt a more emboldened approach in assessing whether the role of the impugned Agreement within the EU Data Protection legal framework is compatible with the EU Charter of Fundamental Rights. Whatever the outcome, such major issues concerning the protection of EU citizens' rights to privacy and data protection would not be before the highest court in the EU if not for the Snowden Revelations which (as highlighted by the Irish High Court) formed the "backdrop" to this latest judicial review.

Finally, it is also important to note that the next test for the commitment of the EU legislature to EU fundamental rights compliance will be the future of the draft EU Directive on Passenger Name Records Directive (PNR Directive). This legislation seeks to harmonize the mass retention of personal data from travel information for law enforcement purposes across the EU. The proposed measure was revised to comply with the standards under Articles 7 and 8 of the EU Charter of Fundamental Rights, following the annulment of the Data Retention Directive by the CJEU in *Digital Rights Ireland and Seitlinger*. Although the European Parliament previously rejected the PNR Directive proposal in 2013, a revised draft of the PNR Directive is currently before the European Parliament (European Parliament, 2015). Although the scope of data retention under the draft Directive has been reduced, its proportionality remains highly suspect given the length of its retention periods—5 years for terrorism offences, 4 years for "serious transnational crime". It will be telling to see how much of a role the Charlie Hebdo attacks in Paris will play in how Parliament responds to the revised draft in this new political context. In other words, will the Parliament ensure that the revised PNR Directive meets the stringent human rights standards set out by the Luxembourg Court in *Digital Rights Ireland and Seitlinger*? Or, is it inevitable that this EU Directive will be subject to challenge for its lack of compliance with the EU Charter of Fundamental Rights before the CJEU in future?

## 5. Conclusion

In the landmark judgment of *Digital Rights Ireland and Seitlinger*, the highest court in the EU rightly erased from the EU legal order the imposition of a mass Internet metadata surveillance regime on Member States that had blatantly disrespected the privacy and data protection rights of more than 500 million EU citizens. This post-Snowden judgment marks the first time that the CJEU has ever struck down an entire EU legal instrument due to its incompatibility with the EU Charter of Fundamental Rights, thereby establishing greater certainty of an EU governed by a fundamental rights culture. Moreover, *Digital Rights Ireland and Seitlinger* established unequivocally that strict legality, necessity and proportionality standards must underpin the protection of privacy and data protection rights in all future EU legislation involving large-scale processing of personal data (including metadata).

Furthermore, the highest court in the EU also surprised EU privacy scholars in its adjudication that data sovereignty forms part of the right to the protection of personal data guaranteed under Article 8 of the EU Charter of Fundamental Rights. To explicitly include a requirement of physical data retention within the EU under the EU Charter may result in major revisions to current provisions and exemptions under EU data protection law. In particular, such a requirement raises questions regarding the processing of data by the private sector and law enforcement authorities outside of the EU—a matter shortly to be before the Luxembourg Court in its review of the EU-US Safe Harbor Agreement. The potential policy implications of the Court's interpretation of Article 8 of the EU Charter in *Digital Rights Ireland and Seitlinger* for the ongoing reform of EU data protection law are of considerable significance to EU and non-EU public and private bodies.

In addition to the striking down of the EU Data Retention Directive in 2014, the CJEU delivered a second landmark privacy judgment shortly thereafter. In *Google Spain*, the Luxembourg Court established that EU citizens have a right to have links concerning them delisted from search engines that essentially encroach upon their private lives and the protection of their personal data. Notwithstanding the understandable concerns raised by freedom of expression advocates prompted by the judgment, it is important to highlight that *Google Spain* was an (albeit ill-conceived) attempt by the Court to address two important problems for the protection of privacy in the 21st century. First, the indefinite and all-encompassing memory of the Internet regarding an individual's personal data and secondly, the enormous influence of search engines regarding an individual's online (and inevitably offline) identity and reputation.

Both of these judgments indicate that the Snowden revelations have been influential in emboldening the highest court in the EU in its review of matters concerning privacy and the processing of personal data by either public or private bodies. In particular, *Digital Rights Ireland and Seitlinger* has contributed to the enhanced protection of privacy and data protection in any future EU legislation involving mass metadata surveillance. Moreover, the influence of the revelations for the protection of information privacy through future judicial review proceedings in Europe may extend further still. Challenges to the compatibility of systems allowing for the covert access and monitoring of communications by US and EU national security and law enforcement authorities with Article 8 ECHR and Article 8 of the EU Charter of Fundamental Rights have been brought before the European Court of Human Rights in Strasbourg, and (again) before the CJEU. Hence, the Snowden revelations seem poised to embolden further jurisprudential developments and debate concerning the future of the legal standards and safeguards essential for the effective protection of privacy and personal data both within and beyond the EU.

## Acknowledgments

I would like to express my thanks to all of my colleagues in the Faculty of Law at the University of Cambridge who shared their insights and observations on the above.

## Conflict of Interests

The author declares no conflict of interests.

## References

Article 29 Data Protection Working Party. (2014). *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*. Brussels: Secretariat of the European Commission.

Computer and Communications Industry Association (CCIA). (2014). CCIA's response to the European Court of Justice Online Privacy Ruling. Retrieved from https://www.ccianet.org/2014/05/ccias-response-to-european-court-of-justice-online-privacy-ruling

Centre for European Legal Studies (CELS). (2015). Podcast of Conference Proceedings "European Internet Regulation after Google Spain". University of Cambridge: UK. Retrieved from https://www.youtube.com/playlist?list=PLy4oXRK6xgzH6JjMA09uPmqOrahpPM9X https://itunes.apple.com/us/itunes-u/eu-internet-regulation-after/id986766672?mt=10 http://sms.cam.ac.uk/collection/1951973

De Vries, K., Bellanova R., De Hert, P., & Gutwirth, S. (2011). The German Constitutional Court judgment on data retention. In S. Gutwirth, Y. Poullet, P. de Hert, & R. Leenes (Eds.), *Computers, privacy and data protection* (pp. 3-23). Dordrecht: Springer.

European Commission. (2005). *Annex to the Extended Impact Assessment: Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC*. COM (2005) 438 final. Brussels: European Commission.

European Parliament. (2015, February 2), *Draft Parliament report on revised PNR directive proposal*. Retrieved from http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE549.223+01+DOC+PDF+V0//EN&language=EN

Fabbrini, F. (2014). Human rights in the digital age. *Tilburg Law School Research Paper Series*, No.15/2014.

FISA Order. (2013). Verizon forced to hand over telephone data—Full court ruling. *The Guardian*. Retrieved from http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order

U.S. Federal Trade Commission (FTC). (2013). *Mobile privacy disclosures: Building trust through transparency*. Washington, DC: FTC.

Gandy, O. H. (2003). Data mining and surveillance in the Post 9/11 Environment. In K. Ball & F. Webster (Eds.), *Intensification of surveillance* (pp. 26-41). London, UK: Pluto.

Granger, M., & Irion, K. (2014). The Court of Justice and the data retention directive in digital rights Ireland. *European Law Review*, *39*(6), 835-850.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA and the U.S. Surveillance State.* London, UK: Picador.

Groussot, X., & Pech, L. (2010). Fundamental Rights Protection in the EU post Lisbon Treaty. *Policy Papers of the Foundation Robert Schuman*, No.173/2010.

Guild, E., & Carrera, S. (2014). The political and judicial life of metadata: Digital rights Ireland and the trail of the data retention directive. *CEPS Paper in Liberty and Security in Europe*, No.65/2014.

Harding, L. (2014). *The Snowden files*. London, UK: Guardian.

Hawkes, B. (2006). The Data Retention Directive and data protection. *Privacy and Data Retention Directive Conference*, Irish Centre for European Law, Ireland. July 19, 2006.

Hayden, M. (2014). The price of privacy: Re-evaluating the NSA. *John Hopkins Foreign Affairs Symposium*. Retrieved from: https://www.youtube.com/watch?v=kV2HDM86XgI

Hayden, M. (2015). Getting past the zero-sum game online. *Washington Post*. Retrieved April 13, 2015 from: http://www.washingtonpost.com/opinions/dont-let-america-be-boxed-in-by-its-own-computers/2015/04/02/30742192-cc04-11e4-8a46-b1dc9be5a8ff_story.html

Kuner, C., Cate, F. H., Millard, C., Svantesson, D. B., & Lynskey, O. (2015). Internet Balkanization gathers pace: Is privacy the real driver? *International Data Privacy Law*, *5*(1), 1-2. doi:10.1093/idpl/ipu032

Kuner, C. (2015). Safe Harbor before the EU Court of Justice. *Cambridge Journal and Comparative Law Journal*. Retrieved from http://cjicl.org.uk/2015/04/13/safe-harbor-before-the-eu-court-of-justice

Lessig, L. (1999). *Code and other law of cyberspace*. New York, US: Basic Books.

Lynskey, O. (2014). The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety. *Common Market Law Review*, 51(6), 1789-1812.

Mayer-Schonberger, V. (2014). Omission of search results is not a "right to be forgotten" or the end of Google. *The Guardian*. Retrieved from http://www.theguardian.com/commentisfree/2014/may/13/omission-of-search-results-no-right-to-be-forgotten

Murphy, C. (2012). *EU counter terrorism law*. Oxford, UK: Hart.

Ni Loideain, N. (2011) Implications of the EC Data Retention Directive for data protection and privacy. In C. M. Akrivopoulou & A. Psygkas (Eds.), *Personal data privacy and protection in a surveillance era: Technologies and practices* (pp. 256-272). Pennsylvania: Information Science Reference.

Ni Loideain, N. (2014a). Surveillance of communications data and Article 8 of the European Convention on Human Rights. In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), *Reloading data protection: Multidisciplinary insights and contemporary challenges* (pp.183-209). London, UK: Springer.

Ni Loideain, N. (2014b). Is the EU really about to outlaw mass metadata surveillance? *Wired.* Retrieved from http://www.wired.co.uk/news/archive/2014-04/28/mass-metadata-surveillance-eu

Schneier, B. (2015). *Data and Goliath: The hidden battles to collect your data and control your world*. New York: W.W. Norton & Company.

Solove, D. J. (2008) *Understanding privacy*. London, UK: Harvard University Press.

Spitz, M. (2012). Your phone company is watching. *TEDGlobal Conference Presentation.* Retrieved from http://www.ted.com/talks/malte_spitz_your_phone_company_is_watching

The President's Review Group on Intelligence and Communications Technologies. (2013). *The NSA report: Liberty and security in a changing world*. Princeton: Princeton University Press.

Wicker, S. B. (2013). *Cellular convergence and the death of privacy*. Oxford, UK: Oxford University Press.

Young, J. M. (2004). Surfing while Muslim: Privacy, freedom of expression and the unintended consequences of cybercrime legislation. *Yale Journal of Law and Technology*, *7*, 346-421.

Zittrain, J. (2014). Don't force Google to forget. *New York Times*. Retrieved from http://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html?_r=0

**About the Author**

**Nóra Ní Loideain**
Nóra Ní Loideain B.A., LL.B., LL.M. (Public Law) is a PhD candidate in Law and CHESS Scholar at the University of Cambridge. Her doctoral thesis concerns the State surveillance of communications metadata in Europe. She is also a Research Associate for the Technology and Democracy Project in the Centre for Research in the Arts, Social Sciences and Humanities at the University of Cambridge. Previously, she was a Policy Officer in the Office of the Director of Public Prosecutions and Clerk for the Supreme Court of Ireland.